

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-159053

(P2002-159053A)

(43) 公開日 平成14年5月31日 (2002.5.31)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームト* (参考)
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 K 0 3 3
9/32			6 0 1 E 5 K 0 6 7
12/28			6 7 5 B
		11/00	3 1 0 B
審査請求 未請求 請求項の数15 O L (全 20 頁)			

(21) 出願番号 特願2000-351066(P2000-351066)

(22) 出願日 平成12年11月17日 (2000.11.17)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 中北 英明

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 高島 由彰

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 100083806

弁理士 三好 秀和 (外7名)

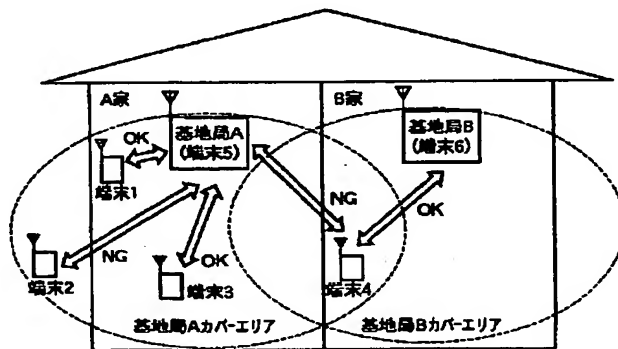
最終頁に続く

(54) 【発明の名称】 無線通信システムで用いられる登録・認証方法

(57) 【要約】

【課題】 無線端末同士や、無線基地局と無線端末との間での登録・認証を、確実かつ容易に実行可能な登録・認証方法を提供する。

【解決手段】 無線基地局、無線端末は、それぞれ、通常モード、登録モード、認証モードからなる3つのモードを有しており、どちらも通常モードから登録モード、認証モード、そして再び通常モードと順に移行することで、無線端末の無線基地局に対する登録・認証処理が実行される。無線基地局、無線端末のモード移行の一部について利用者からのマニュアル操作を要求することで、正当ではない利用者による無線端末の登録・認証を抑制する。



**【特許請求の範囲】**

**【請求項 1】** 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(c) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；

(d) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

(e) 前記無線端末のモードが認証モードに移行した後、前記無線基地局が前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(f) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(g) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

**【請求項 2】** 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り

替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(c) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(d) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

(e) 前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを登録モードから認証モードに切り替えると共に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(f) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(g) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

**【請求項 3】** 前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第 1 の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第 2 の時間経過までに前記無線端末から前記認証受領情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、

前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第 3 の時間経過までに前記無線基地局から前記登録確認情報を受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第 4 の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項 1 または 2 に記載の登録・認証方法。

**【請求項 4】** 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから

成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(c) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；

(d) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

(e) 前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線端末を操作することで、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；

(f) 前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(g) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(h) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項5】 前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第1の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第2の時間経過までに前記無線端末から前記認証申請情報および認証受領情報のうちのいずれかを受信できない場合には、前記無線端

末の前記無線基地局に対する登録・認証処理を中止し、前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第3の時間経過までに前記無線基地局から前記登録確認情報を受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第4の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項4に記載の登録・認証方法。

【請求項6】 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；

(c) 前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(d) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；

(e) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替えると共に、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；

(f) 前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(g) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(h) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項7】 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；

(c) 前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(d) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段階；

(e) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

(f) 前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線端末を操作することで、前記無線端末の前記無線基地局に対する認証申請を示す認証申請情報を前記端末秘密鍵および端末暗号方式を用いて暗号化して前記無線基地局に送信する段階；

(g) 前記暗号化された認証申請情報を前記無線基地局が前記端末公開鍵を用いて復号できた場合に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(h) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(i) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項8】 前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第1の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第2の時間経過までに前記無線端末から前記認証申請情報および認証受領情報のうちのいずれかを受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第3の時間経過までに前記無線基地局から前記登録受付情報および登録確認情報のうちのいずれかを受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第4の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項6または7に記載の登録・認証方法。

【請求項9】 無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、次の工程を含むことを特徴とする登録・認証方法。

(a) 利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替える段階；

(b) 前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替えると共に、前記無線基地局に対する登録受付可能を示す登録受付情報を前記無線端末に送信する段階；

(c) 前記無線端末が前記登録受付情報を受信すると、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；

(d) 前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(e) 前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；

(f) 前記無線端末のモードが認証モードに移行した後、前記利用者が前記無線基地局を操作することで、前記無線基地局のモードを登録モードから認証モードに切り替えると共に、前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；

(g) 前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；

(h) 前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階

【請求項10】 前記無線基地局は、前記無線基地局のモードが通常モードから登録モードに切り替わった時点から予め定められた第1の時間経過までに前記無線端末から前記登録申請情報を受信できない場合、あるいは前記無線基地局のモードが登録モードから認証モードに切り替わった時点から予め定められた第2の時間経過までに前記無線端末から前記認証受領情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止し、

前記無線端末は、前記無線端末のモードが通常モードから登録モードに切り替わった時点から予め定められた第3の時間経過までに前記無線基地局から前記登録受付情報および登録確認情報のうちのいずれかを受信できない場合、あるいは前記無線端末のモードが登録モードから認証モードに切り替わった時点から予め定められた第4の時間経過までに前記無線基地局から前記認証通知情報を受信できない場合には、前記無線端末の前記無線基地局に対する登録・認証処理を中止することを特徴とする請求項9に記載の登録・認証方法。

【請求項11】 前記無線端末は、前記無線基地局に対する登録・認証処理が完了した場合には、前記無線端末が登録済みであることを特定する通常モードに移行することを特徴とする請求項1乃至10に記載の登録・認証方法。

【請求項12】 前記無線端末は、通常モード、登録モードおよび認証モードのうちのいずれかを設定する状態設定部と、前記状態設定部によって設定されたモードを利用者に表示する状態表示部と、前記端末公開鍵、端末秘密鍵および端末暗号方式を予め保持する端末情報管理部と、取得した前記基地局鍵および基地局暗号方式を格納するシステム認証情報管理部とを備え、前記状態設定部は、前記利用者からモード移行要求を入力した場合には、該モード移行要求にしたがうことを特徴とする請求項1乃至11に記載の登録・認証方法。

【請求項13】 前記無線端末は、更に、前記第3および第4の時間を管理するタイマ設定部を備えることを特徴とする請求項3、5、8または10に記載の登録・認証方法。

【請求項14】 前記無線基地局は、通常モード、登録モードおよび認証モードのうちのいずれかを設定する状

態設定部と、前記状態設定部によって設定されたモードを利用者に表示する状態表示部と、前記基地局共通鍵および基地局暗号方式を予め保持するシステム認証情報管理部と、取得した前記端末鍵および端末暗号方式を格納する端末認証情報管理部とを備え、前記状態設定部は、前記利用者からモード移行要求を入力した場合には、該モード移行要求にしたがうことを特徴とする請求項1乃至11に記載の登録・認証方法。

【請求項15】 前記無線基地局は、更に、前記第1および第2の時間を管理するタイマ設定部を備えることを特徴とする請求項3、5、8または10に記載の登録・認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、無線LANを用いた無線通信システム、この無線通信システムを構成する無線端末、無線基地局、この無線通信システムの登録・認証方法に係り、特に、IEEE802.11等の無線LANシステムにおける、無線端末同士や、無線基地局と無線端末との間の、登録・認証技術に関する。

【0002】

【従来の技術】近年のLAN(Local Area Network)技術の発達に伴い、オフィス環境のネットワーク化がPC(Personal Computer)間の接続を中心として進行している。このような有線LANの普及の一方で、有線LANの一部分を無線で置換する無線LAN化も進んでいる。たとえば、有線LANに無線基地局を接続し、この基地局へ複数の携帯型PCを無線で接続する場合である。この携帯型PCを用いて有線LANにイーサネット（登録商標）接続されているデスクトップPCのファイルを編集すれば、有線LANへ無線アクセスを行っていることになる。また、基地局と携帯型PCの部分の切り出してみると、その部分は無線LANを形成している。このような無線LANの利点としては、伝送路として電波や赤外線などを利用するので配線敷設が不要な点や、ネットワークの新設やレイアウト変更が容易な点が挙げられる。

【0003】このような無線LANの導入はIEEE802.11の標準化によって拍車がかかっている。IEEE802.11では、1997年に2.4GHz帯の無線LAN仕様を、1999年に5GHz帯の無線LAN仕様を、それぞれ完成させている。2.4GHz帯の無線LAN仕様の伝送速度は、1~2Mbpsのものと11Mbpsのものがあり、さらに、20Mbpsを超える仕様が現在検討中である。最近、この2.4GHz帯仕様に準拠した製品が、各社から発売されるようになり、基地局や無線PCカードが普及価格帯に入りつつある。一方、5GHz帯の無線LAN仕様では、20~30Mbpsの伝送速度を実現可能である。また、5GHz帯は2.4GHz帯とは異なり、現在は気象レーダに



利用されているだけのほぼ未使用な周波数帯域であり、かつ、より高速な伝送速度が容易に見込めるため、次世代の無線LAN仕様と期待されている。

【0004】また、ここに来て、Bluetoothが携帯電話業界や、家電業界、PC業界を巻き込んで、あらゆる機器に搭載されようとしている。このBluetoothも2.4GHz帯の無線システムであるが、1チップ5ドル程度という低コストと、幅広い業種の約2000社から賛同を得ていることから、世界的な普及が見込みに見込まれている。

【0005】以上のような状況から、無線LANシステムはオフィス環境だけでなく、一般家庭にも普及が進んでいくものと考えられる。したがって、近い将来、複数の無線LANシステムが隣接するとか、同一空間に共存するというような環境が広く築かれると予想される。

【0006】ところで、IEEE802.11では、無線端末間や、無線基地局と無線端末との間の認証処理が規定されている（IEEE802.11仕様書の第8章）。この規定では、認証処理の対象となる2つのエンティティ（無線端末同士、または、無線基地局と無線端末）が、同一の秘密鍵（共通鍵）を使用して認証し、かつ、秘匿通信する方式が記述されている（ただし、この認証処理はオプション扱いである）。この認証処理には、WEP(Wired Equivalent Privacy)と呼ばれるアルゴリズムが用いられる。秘密鍵の配布はあらかじめセキュアな方法で行われる、とだけ記載されている。また、秘密鍵は2つのエンティティそれぞれに対応するので、或る無線端末から見れば、システム内の他の無線端末ごとにも秘密鍵を有する必要がある、システム全体では無線端末数の二乗オーダーの秘密鍵が必要とされる。

【0007】ここで、WEPアルゴリズムによる暗号化と復号化に簡単に触れる。そして、このWEPアルゴリズムを用いた認証についても記述する。図31は、IEEE802.11のWEPアルゴリズムの暗号化処理の説明図である。図31では、送信されるデータが暗号化される処理が示されており、特に、その送信されるデータをここでは平文PTと呼ぶ。

【0008】まず、送信側において、このPTからCRCが生成される。すなわち、ICVが生成される。一方、秘密鍵Skと初期ベクトルIVとから、WEP乱数発生器を経て、キーシーケンスKSが生成される。このKSは、PTとICVとの連結結果{PT, ICV}と長さを合わせた上で、排他的和算される。この排他的和算の結果が暗号文ETである。そして、このETとIVに制御コードを合わせることで、図32に示すWEPフレームを構成する。このWEPフレームによって、WEPアルゴリズムによる秘匿通信が行われる。

【0009】図33に、IEEE802.11のWEPアルゴリズムの復号化処理の内容を示す。図33では、受信された暗号化データを復号化する処理が示されてい

る。図33において、受信側がWEPフレームを受信すると、そのWEPフレームからIVを取り出し、秘密鍵Skと共にWEP乱数発生器に入力し、キーシーケンスKSを発生させる。このキーシーケンスKSは、IVが改竄されていないならば、図31のKSと同じものが生成されるはずである。このKSをフレーム内の暗号文ETと排他的和算すれば、平文PTとICVが復号される。このPTをCRCチェックし、その結果であるICV'と復号されたICVとを比較することで、PTの正しさを確認する。ICV'とICVが等しければ、PTの受信に成功したことになる。

【0010】図34に、IEEE802.11のWEPアルゴリズムによる認証処理のシーケンスチャートを示す。図34は、無線基地局（基地局）とこの基地局の無線ゾーン内の無線端末（端末）との間で無線通信する例を示している。図34において、共通鍵である秘密鍵Skは、基地局と端末との間であらかじめ互いに交換されている（ステップS1001）。そして、まず最初に、端末が基地局へ無線通信で認証要求のフレームを送る（ステップS1002）。この認証要求フレームには、共通鍵方式による認証を要求していることが記入される。なお、上記のステップS1001で、秘密鍵Skは、基地局および端末の双方へ配布済みである。

【0011】次に、基地局は、認証要求受理のステータスにあれば、この秘密鍵Skと内部で発生させた初期ベクトルIVから、WEP乱数発生器を経て、試験文CTを作成する（ステップS1003）。通常、このCTの長さは128バイトである。基地局は、作成したCTを端末へ無線通信する（ステップS1004）。

【0012】端末は、基地局から受け取ったCTを平文として扱い、上記の図31に示した方法により秘密鍵Skで暗号化する（Sk(CT)）（ステップS1005）。そして、このSk(CT)を含む暗号文を、端末が基地局へ無線通信する（ステップS1006）。

【0013】最後に、端末から送られて来た暗号文が基地局で検証され（ステップS1007）、正しければ、端末に向けて、成功ステータスの認証完了フレームが送られる。一方、正しくなければ、失敗ステータスのフレームが送られる（ステップS1008）。この検証は、上記の図33で示した方法でSk(CT)を復号した結果であるSk(Sk(CT)) (=CT')と基地局が最初に作成したCTとが同一であるかを調べることによって実行される。

【0014】

【発明が解決しようとする課題】上述したように、無線LANシステムの普及に伴って、一般の家庭内で、複数の無線LANシステムが隣接したり、同一空間に共存したりする場合があります。ここで、図1に例示する、集合住宅内の隣接した2軒の家、A家およびB家それぞれに家庭内無線通信システムが設置されている場合を考

えてみる。

【0015】図1の例では、A家に無線基地局Aが、B家に無線基地局Bがそれぞれ設置されている。しかしながら、基地局A、Bのカバーエリアは、それぞれの基地局A、Bが設置された家A、Bからはみ出してしまいう可能性が十分にある。たとえば、A家の基地局Aから見れば、A家に属する端末1、3のみならず、屋外の端末2や、B家の端末4も、基地局Aのカバーエリア内に存在してしまっている。しかしながら、屋外の端末2、B家の端末4は、A家に属する端末ではないので、基地局Aは端末2、4から登録・認証要求があっても、端末2、4には認証を与える必要はない。すなわち、基地局Aが認証すべき端末は、A家の端末である端末1、3だけである。したがって、基地局Aは、A家の端末1、3以外に認証を与えないように、端末の登録・認証を管理するようにしたい。B家の基地局Bにおいても、同様のことが言える。

【0016】さらに、家庭内の機器には、異なる製造メーカー間であっても、機器同士の相互接続性が要求される。メーカー独自仕様が許容されるIEEE802.11のような無線LANでは、秘密鍵の配布は、図34のステップS1001で行えば良い。たとえば、あらかじめ秘密鍵を基地局や端末に作り込んでおけば良い。しかしながら、家庭内無線通信システムでは、無線によるセキュアかつ容易な方法で、異なるメーカーの装置間で秘密鍵を交換できる仕組みが別途必要となる。

【0017】本発明は、かかる事情に鑑みて成されたものであり、その目的は、IEEE802.11等の無線通信システムであって、無線端末同士や、無線基地局と無線端末との間での登録・認証を、確実かつ容易に実行可能な無線通信システムを提供することである。

【0018】

【課題を解決するための手段】ここで開示される発明のうち代表的なものの概要を説明すれば次の通りである。すなわち、無線基地局と、該無線基地局に登録・認証済みで該無線基地局と無線通信を行う無線端末とから成る無線通信システムにおける、前記無線端末の前記無線基地局に対する登録・認証方法において、(a)利用者が前記無線基地局を操作することで、前記無線基地局のモードを通常モードから登録モードに切り替える段階；

(b)前記利用者が前記無線端末を操作することで、前記無線端末のモードを通常モードから登録モードに切り替えると共に、前記無線端末に固有の公開鍵、該公開鍵の暗号方式および前記無線端末の識別番号を含む登録申請情報を前記無線端末から前記無線基地局に送信する段階；(c)前記無線基地局が前記登録申請情報を受信すると、前記無線端末の登録許可を示す登録確認情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信し、前記無線基地局のモードを登録モードから認証モードに切り替える段

階；(d)前記暗号化された登録確認情報を前記無線端末が前記端末公開鍵に対応する端末秘密鍵を用いて復号できた場合に、前記無線端末のモードを登録モードから認証モードに切り替える段階；(e)前記無線端末のモードが認証モードに移行した後、前記無線基地局が前記無線基地局に固有の共通鍵、該共通鍵の暗号方式および前記無線基地局の識別番号を含む認証通知情報を前記無線基地局が前記端末公開鍵および端末暗号方式を用いて暗号化して前記無線端末に送信する段階；(f)前記暗号化された認証通知情報を前記無線端末が前記端末秘密鍵を用いて復号できた場合に、前記認証通知情報の受領を示す認証受領情報を前記無線端末が前記基地局共通鍵および基地局暗号方式を用いて暗号化して前記無線基地局に送信し、前記無線端末のモードを認証モードから通常モードに切り替える段階；(g)前記暗号化された認証受領情報を前記無線基地局が前記基地局共通鍵を用いて復号できた場合に、前記無線基地局のモードを認証モードから通常モードに切り替える段階、を含む登録・認証方法であることである。

【0019】本発明に係る登録・認証方法では、たとえば家庭内に設置された無線基地局に対して無線端末の登録・認証を行う場合、無線端末の利用者は無線基地局を直接操作しなければならない。このため、無線基地局の操作が容易でない外部の利用者の無線端末の登録・認証を防止できる。それにより、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実現できる。

【0020】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。本発明の主な対象は、家庭内無線通信システムである。このシステムでは、管理上は無線基地局が無線端末の登録および認証を行い、通常のデータ通信が端末間で直接行われる。端末は、公開鍵暗号方式による暗号方式と、その秘密鍵および公開鍵を持つことが前提である。公開鍵暗号方式としては、たとえば、RSA暗号方式や楕円暗号方式が挙げられる。基地局は、共通鍵暗号方式による暗号方式と、その共通鍵を持つことが前提である。共通鍵暗号方式としては、たとえば、DES方式やAES方式などが挙げられる。

【0021】本発明では、まず、端末の公開鍵暗号方式で登録を行い、次に、基地局の共通鍵暗号方式で認証を行う。したがって、本発明は、通常のデータと同じ無線通信方式を用いて、基地局が端末を登録および認証し、その結果、認証を受けた端末同士は、基地局管理の共通鍵方式でシステム内秘匿通信をすることができる。本発明によって、認証を受けていない外部端末が、システム内の通信を傍受することや、システム内の端末としてなりすましを防止できる。また、本発明は、IEEE802.11のWEPアルゴリズムにおいて前提となっているデータ通信用秘密鍵の事前配布方法として使用するこ

とも可能である。この場合には、本発明方式の利用後、WEPアルゴリズムで、IEEE 802.11としての端末認証を行うことになる。

【0022】基地局は、家庭内無線通信システムの管理上の責任を負うだけで、それ以外の機能は他の端末と何ら変わらない。逆に言うと、端末の登録・認証機能を基地局機能と呼ぶことにすると、この基地局機能をもつ端末が基地局になることも可能であり、この考え方はIEEE 1394にも通ずるものである。このため、たとえば、図1に示すように、基地局Aを「端末(端末5)」、基地局Bを「端末(端末6)」として扱うこともできる。

【0023】以下、本発明の実施の形態に係る無線通信システムについて6つの実施例を用いて説明する。第1乃至第6の実施例は、それぞれ、図1の基地局Aに端末1を登録および認証する場合を示している。本発明の特徴は、利用者が、端末および基地局の両方を操作しながらそれぞれの状態を確認しつつ、端末の登録・認証を進めていく点にある。このため、無線通信によりながらも、セキュアかつ容易に、端末の登録・認証を実現できる。すなわち、端末や基地局の操作を利用者に要求することで、利用者はボタンを押す順序などのシーケンスに正しく従う必要がある。また、外部から家屋内の基地局Aをマニュアル操作することは困難である。このため、たとえば、図1の端末2や端末4が基地局Aに登録することは基本的に不可能である。万が一、これら外部の端末2、4を、A家の端末1あるいは端末3の登録・認証のときに、横槍を入れて登録・認証させようとしても、基地局Aや端末1あるいは端末3の状態表示で、そのような動作をA家の利用者は簡単に検出することができる。

【0024】(第1の実施例)次に、図2および図3を用いて、本発明の実施の形態に係る無線通信システムの第1の実施例を説明する。図2は、この第1の実施例に係る無線通信システムの登録・認証シーケンスチャートである。ここでは、図1の基地局A(端末5)と端末1との間での登録・認証シーケンス(登録・認証シーケンス1)が示されている。この登録・認証シーケンス1は、大きく分けて、登録段階と認証段階とに分けられる。なお、図2では、時刻 $t$ は上から下に経過していくものとする。これらは、後述の他の実施例のシーケンスにおいても同様である。図3は、基地局Aと端末1との間で交換される情報に焦点をあてて、図2の登録・認証シーケンス1を説明するものである。図3に示された丸囲み数字は、登録・認証シーケンス1の進行順を示している。この登録・認証シーケンス1では、端末1から基地局Aへ登録申請情報および認証受領情報が無線通信される。また、基地局Aから端末1へ登録確認情報および認証通知情報が無線通信される。以下、図2を参照して、この登録・認証シーケンス1を説明する。

【0025】基地局Aは、①通常モード、②登録モード、および、③認証モードを有している。また、端末1も、①2種類の通常モード、すなわち、未登録通常モードと登録済み通常モード、②登録モード、および、③認証モードを有している。もちろん、基地局Aと同様、通常モードは1種類であっても構わない。通常モードが2種類の場合、端末1の登録は1回だけに限定され、結果として、1基の基地局だけに登録可能となる。一方、通常モードが1種類の場合には、複数の基地局に登録することができる。端末1の登録が1回に限定されないからである。なお、図2では、基地局Aおよび端末1のLED表示について次の表記を用いる。「R」は赤色点灯で、登録モードを表す。「G」は緑色点灯で、登録済み通常モードを表す。「<R>」は赤色点滅で、認証モードを表す。「<G>」は緑色点滅で、未登録通常モードを表す。なお、LED表示の例は、他にもバリエーションが考えられる。たとえば、認証モードは黄色点灯などである。また、図2の基地局A、端末1の直角三角形表示は、利用者によるボタン操作を表している。

【0026】(a)まず、利用者は、基地局Aの登録ボタンの操作によって、基地局Aのモードを通常モードから登録モードに切り替える(時刻a、ステップS101)。また、この時、タイマ1がスタートする。

【0027】(b)次に、利用者は、端末1の登録ボタンを押す(時刻b、ステップS102)。その操作に応じて、端末1は基地局Aに登録申請情報を無線送信する(ステップS103)。また、端末1の登録ボタンが押された時点で、タイマ3がスタートする。この登録申請情報の送信の後、端末1のモードも通常モードから登録モードに切り替わる。この時点で、基地局Aと端末1の両方が登録モードに移行したことになる。

【0028】端末1が送信する登録申請情報には、図4に示すように、端末1のMACアドレス、端末1の公開鍵および公開鍵暗号方式、その他端末1固有の情報(機器種別、シリアル番号、製造会社名、利用者氏名等)が含まれる。MACアドレスとしては、IEEEのEUI 64アドレスまたはEUI 48アドレスが考えられる。これらのアドレスによれば、端末1を一意に特定できるからである。EUI 64アドレスは、前半の24ビットと後半の40ビットに分けられ、前半部分がIEEEによって割り当てられるCompany IDで、後半部分はこのCompany IDが割り当てられた会社が自由に使用することができる。たとえば、AC-DE-64-00-00-00-00-80(ヘキサ表示)というアドレスが示される。IEEE 1394ではノード(端末)固有のアドレスとしてEUI 64を用いる。EUI 48アドレスはイーサネットアドレスなどで使用されており、後半部分が24ビットである点を除けば、EUI 64とほぼ同じである。また、EUI 64アドレスで、後半部分の最初の2オクテットをFF-FE(ヘキサ表



示)に設定すれば、EUI48アドレスフォーマットとして使用することができる。

【0029】公開鍵および公開鍵暗号方式は、端末1があらかじめ保有しているものである。これらは、たとえば、製品出荷時に端末1自身に搭載されたROMなどに書き込まれたり、端末1の無線インタフェースカードのROMに書き込まれたりする。

【0030】端末1固有情報の例としては、機器の種別やシリアル番号や製造会社名、利用者の氏名などの情報が考えられる。これらの情報はコード化して管理してもよい。たとえば、機器種別を4ビットで表現して、0000がワイヤレスTV、0001がデジタルVCR、0010がノートPCなどと決めておけば良い。製造会社名も、00000が東芝、00001がソニーなどとあらかじめ割り当てておけば良い。

【0031】(c) 基地局Aは、端末1からの登録申請情報を受理した場合、端末1へ登録確認情報を返す(時刻c、ステップS104)。この登録確認情報は、基地局A側で端末1を登録することができたことを端末1側に報告するものである。この時、基地局Aのモードが登録モードから認証モードに切り替わる。また、タイマ2もスタートする。登録確認情報は、登録申請情報によって端末1から受理した端末1の公開鍵により暗号化されている。この暗号化によって、登録申請を要求した端末1だけが登録確認情報の中身を読むことができる。この登録確認情報には、図5に示すように、登録がOKであることを示すフラグ、登録OKの対象である端末1のMACアドレス、端末固有情報などが含まれる。これらの端末MACアドレスや端末固有情報などは、上記の図4の登録申請情報から得られるものである。

【0032】(d) 基地局Aからの登録確認情報の受理によって、端末1のモードが、登録モードから認証モードに切り替わる(時刻d)。この時、タイマ4がスタートする。

【0033】(e) 認証モードへの移行時点(時刻c)からあらかじめ定められた時間経過後、基地局Aは認証通知情報を端末1へ送信する(時刻e、ステップS105)。この時刻eと時刻dとの関係は、端末1が確実に認証モードにある時に認証通知を受信できるように配慮される。認証通知情報には、図6に示すように、認証通知、基地局AのMACアドレス、基地局Aの共通鍵と共通鍵暗号方式、そして、基地局Aの固有情報が含まれる。そして、登録確認情報と同様に、端末1の公開鍵および公開鍵暗号方式を用いて暗号化されている。端末1だけが公開鍵と対の秘密鍵を持っているので、それ以外の端末は端末1への認証通知情報を確認することができない。

【0034】(f) 端末1が認証通知情報を受理すると、認証受領情報を基地局Aへ返信する(時刻f、ステップS106)。この時、端末1のモードは、認証モー

ドから通常モード(緑色点灯表示)に切り替わる。登録および認証処理の当初、未登録通常モード(緑色点滅)だった端末1は、登録済み通常モード(緑色点灯)となる。一方、当初は通常モード(緑色点灯表示)だった基地局Aは、元に戻る。認証受領情報は、図7に示すように、端末1が認証通知を受領したこと(認証OK)を、端末1の端末アドレスや基地局MACアドレスとともに含むものである。これらは、基地局Aの共通鍵および共通鍵暗号方式で暗号化され、基地局Aへ送信される。

【0035】(g) 基地局Aは、端末1からの認証受領情報を正しく復号できた場合に、認証モードから通常モードに戻る(時刻g)。この時、時刻gで端末1も基地局Aも通常モードになっている場合、この端末1は基地局Aに登録・認証され、処理が完了する。

【0036】このようにして登録・認証された端末1は、基地局Aが管理する家庭内無線通信システムの中で、基地局Aの共通鍵暗号方式を利用することが可能となり、他の認証済み端末と秘匿通信できるようになる。たとえば、図8に示すように、端末間通信データが秘匿される。すなわち、図8は、基地局Aが家庭内無線通信システム管理している例で、基地局Aがあらかじめ保持する共通鍵SKsaおよびその暗号化方式SAsaを用いて暗号化している。この場合、基地局Aから登録・認証を受けない限り、この秘匿通信データを各端末は読むことができない。

【0037】図9は、基地局Aによって管理される登録認証テーブルの内容を示す図である。この登録認証テーブルには、端末ごとに、MACアドレス、公開鍵、暗号方式、端末固有情報などが記録されている。これらの端末ごとのデータは、上記の図4に例示した、各端末の登録申請情報から得られる。もちろん、このテーブルには基地局A自身の情報も含まれる。基地局A自身の情報としては、基地局Aがあらかじめ保持する共通鍵およびその共通鍵暗号方式が挙げられる。さらに、基地局Aが端末として機能する際に必要な情報である、MACアドレス、公開鍵暗号方式による公開鍵、秘密鍵およびその暗号方式、他の端末固有情報も含まれる。

【0038】上記の第1の実施例では、図2のタイマ(タイマ1～タイマ4)を用いて、登録・認証の失敗をハンドリングし、基地局Aや端末1を通常モードに戻すことが可能である。以下、この際のタイマの動作について、図10乃至図14を用いて説明する。

【0039】(1) 図10は、端末1が登録申請情報を基地局Aへ送信したが、基地局Aがこの情報をうまく受信できず、その結果、登録確認情報を返信できなかった場合のシーケンスチャートである。この場合、基地局Aでは、時刻aでタイマ1がスタートしたが、時刻cで時間切れになり、元の通常モードに戻る。一方の端末1も、時刻bでタイマ3がスタートしたが、登録申請情報の返事、すなわち、登録確認情報をもらえないまま、時

刻dに時間切れとなり、元の通常モードに戻る。基地局Aも端末1も、認証モードに入らずに通常モードに戻る。失敗したことは視覚的に判断できる。また、タイマ1とタイマ3の制限時間を登録・認証に要する時間よりも長めに設定しておけば、その時間の長さも視覚的判断材料とすることができる。

【0040】(2)図11は、端末1が基地局Aからの登録確認情報を正しく復号できなかった場合のシーケンスチャートである。この場合、端末1は登録確認情報を正しく受け取ることができないため、タイマ3が時間切れとなり、端末1のモードは元の通常モードに戻ってしまう。その結果、基地局Aは、端末1から認証受領情報を受け取ることができないので、同様にタイマ2が時間切れとなり、基地局Aのモードも元の通常モードに戻ることになる。

【0041】なお、基地局Aのタイマ1は登録確認情報を端末へ送出した時刻cに正常に解除される。

【0042】(3)図12は、端末1が基地局Aからの認証通知情報を正しく受け取れなかった場合のシーケンスチャートである。すなわち、上記の図2に示したように、通常、タイマ2のスタート時刻cから一定時刻経過後、基地局Aは認証通知情報を端末1へ送信することになっている。しかしながら、この認証通知情報の端末1への送信が何らかの理由で失敗する場合が想定される。この場合、基地局Aは、認証通知情報の受信失敗の結果として、端末1から認証受領情報を受け取ることができない。このため、タイマ2は時間切れとなり、基地局Aのモードは元の通常モードに戻ることになる。一方、端末1は、基地局Aから認証通知情報を受信できず、タイマ4が時間切れとなって、元の通常モードに戻る。

【0043】なお、基地局Aのタイマ1は、登録確認情報を端末1へ送出した時刻cで、正常に解除されている。また、端末1のタイマ3も、登録確認情報を正しく復号できた時刻dで、正常に解除されている。

【0044】(4)図13は、端末1が基地局Aからの認証通知情報を正しく復号できなかった場合のシーケンスチャートである。この場合、端末1は、上記の(3)の場合と同様、基地局Aから認証通知情報を正しく受け取ることができない。このため、タイマ4が時間切れとなって、端末1は元の通常モードに戻る。一方、基地局Aも、上記の(3)と同様、端末1から認証受領情報を受信できず、タイマ2が時間切れとなり、元の通常モードに戻る。

【0045】なお、基地局Aのタイマ1は、登録確認情報を端末1へ送出した時刻cで、正常に解除されている。また、端末1のタイマ3も、登録確認情報を正しく復号できた時刻dで、正常に解除されている。

【0046】(5)図14は、基地局Aが端末1からの認証受領情報を正しく復号できなかった場合のシーケンスチャートである。この場合、基地局Aは、端末1から

の認証受領情報を復号できないので、タイマ2が時間切れとなり、元の通常モードに戻る。一方、端末1は、基地局Aからの認証通知情報を正しく受信できたので、正常な動作として、元の通常モードに戻る。また、基地局Aの認証受領情報の復号失敗は、タイマ2の時間切れによって検出されることになる。このタイマ2の制限時間を正常終了時よりも長く設定した場合には、基地局Aの認証モードに滞在する時間の増大によって、認証受領情報の復号か失敗を判断できる。

【0047】なお、基地局Aのタイマ1は、登録確認情報を端末1へ送出した時刻cで、正常に解除されている。また、端末1のタイマ3も、登録確認情報を正しく復号できた時刻dで、正常に解除されている。さらに、端末1のタイマ4も認証受領情報を基地局Aへ送出した時刻fで、正常に解除されている。

【0048】上記の(1)乃至(4)において、端末1の通常モードが未登録通常モードと登録済み通常モードに分かれている場合は、登録・認証に失敗した時、端末1が未登録通常モードに戻るようになる。この場合には、通常モードが1つの場合と比べて、利用者がより視覚的に判断することが可能となる。

【0049】上記の第1の実施例では、1つの登録・認証シーケンスによっては1つの端末しか登録・認証を受けることができない。以下、この点について、図15を用いて説明する。図15の例では、端末2の方が端末1よりも早く登録ボタンを押したため(ステップS102、ステップS102')、端末2の登録申請情報が受理され(ステップS103、ステップS103')、その結果として登録・認証を受けることができた。一方の端末1は、登録ボタンを押した時点t<sub>s</sub>から、登録モードであったが、時刻t<sub>e</sub>でタイマ1が時間切れとなり通常モードに戻っている。このタイマ1の時間切れと、認証モードに入らなかったことから、端末1の登録・認証失敗が判断できる。このように、基地局が、登録申請情報を登録モード期間中だけ受け付け、かつ、1つの端末からの登録・認証要求だけしか受け付けないことにすると、端末の登録・認証は、同時には1つの端末だけであることが保証されることになる。これによれば、他家もしくは外部の端末を誤って登録・認証したことも推定できるので、端末の登録・認証をやり直すことができる。たとえば、図15の端末1が内部端末、端末2が外部端末であるとする。この場合、内部端末1が失敗したにも関わらず、基地局が正しいシーケンスを辿っていることが一目瞭然なので、何らかの端末(ここでは、外部端末2)が誤って登録・認証された可能性があると判断できる。このように判断できることにより、内部端末1の登録・認証をやり直したり、基地局の登録認証テーブル(図9参照)を修正したりすることが可能である。基地局の登録認証テーブルの修正は、最新情報のみの削除や全情報の削除などが行える。

【0050】また、上記の第1の実施例において、図2の登録確認情報の送信（ステップS104）と認証通知情報の送信（ステップS105）とを兼ねてしまうシーケンスも考えられる。この場合には、基地局Aは、端末1からの登録申請情報を受理した時、図5の登録確認情報と図6の認証通知情報とを結合し、端末1の公開鍵暗号方式の公開鍵と暗号化アルゴリズムとにより暗号化した後、返信することになる。この登録確認・認証通知を受理した時に、端末1のモードは認証モードに移行する。この認証モードの最中に認証受領情報を作成する。そして、認証受領情報を基地局Aへ送信したとき、端末1は通常モードに切り替わる。

【0051】以上説明したように、上記の第1の実施例によれば、基地局Aの登録ボタンを操作してから、基地局Aのタイマ1がタイムアウトする前に、端末1の登録ボタンを操作する必要がある。このため、家屋内にある基地局Aを外から操作することが困難なことに合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0052】（第2の実施例）次に、図16および図17を用いて、本発明の実施の形態に係る無線通信システムの第2の実施例を説明する。図16は、この第2の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図16の登録・認証シーケンス（登録・認証シーケンス2）が上記の第1の実施例の登録・認証シーケンス1と異なる点は、時刻eで基地局Aが認証通知情報を送る際（ステップS206）、明示的に認証ボタンを押す点である（ステップS205）。この認証ボタンは、登録ボタンと別々に配置しても良いし、同一ボタンであっても良い。同一のボタンで構成する場合には、短く（たとえば1秒以内）押したとき登録ボタンで、長く（たとえば数秒）押したとき認証ボタンとしてもよい。このほかにも様々なバリエーションが考えられる。いずれにせよ、このように認証ボタンを利用すると、端末が登録モードから認証モードに変わったことを利用者が確認した後に、明示的に認証ボタンで認証動作をスタートさせることができる。したがって、上記の第1の実施例の登録・認証シーケンス1よりも、登録段階が終了して認証段階に入ったことを、利用者が容易に認識できる。

【0053】図16のタイマ（タイマ1、タイマ2、タイマ3、タイマ4）は、タイマ2のスタートが異なる点を除いて、図2の登録・認証シーケンス1と同様である。また、タイマの用途も、シーケンス1と同様で、図10乃至図14と同様に動作する。図16の基地局Aのタイマ2は、基地局Aの認証ボタンを利用者が押した時点からスタートする。認証受領情報を正しく復号できた時に解除され、それ以外の異常時には制限時間を越えたところで解除される。

【0054】図17は、基地局Aと端末1との間で交換

される情報に焦点をあてて、図16の登録・認証シーケンス2を説明するものである。図17の丸囲み数字は登録・認証シーケンス2の進行順を示すものである。この登録・認証シーケンス2では、端末1から基地局Aへ登録申請情報および認証受領情報が無線通信される。一方、基地局Aから端末1へ登録確認情報および認証通知情報が無線通信される。

【0055】この第2の実施例は、上記の第1の実施例と比べて、認証通知と端末の認証モードへの切り替わりとの相関が明確なため、所望でない端末の誤った登録・認証を防止できる点が有利である。第1の実施例で述べた図11、図13、図14の例では、端末1の登録・認証の失敗は、別の端末が誤って登録・認証されたことが原因である可能性もある。これは、基地局Aからの認証通知の返信タイミングを端末1が把握できないためである。これに対し、この第2の実施例では、端末1が認証モードになったことを確認してから、利用者が基地局Aの認証ボタンを操作するため、この返信タイミングは明確である。したがって、基地局Aが別の端末を誤って登録・認証してしまうことを防止できる。

【0056】以上説明したように、この第2の実施例によれば、基地局Aの登録ボタンを操作してから、基地局Aのタイマ1がタイムアウトする前に、端末1の登録ボタンを操作する必要がある。また、端末1が認証モードに切り替わった後、基地局Aの認証ボタンを操作する必要がある。このため、家屋内にある基地局Aを外から操作することが困難なことに合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0057】（第3の実施例）次に、図18および図19を用いて、本発明の実施の形態に係る無線通信システムの第3の実施例を説明する。図18は、この第3の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図18の登録・認証シーケンス（登録・認証シーケンス3）が上記の第2の実施例の登録・認証シーケンス2と異なる点は、基地局Aの認証ボタンではなく、端末1の認証ボタンを、利用者が明示的に押す点である（ステップS305）。このようにすると、端末1が登録モードから認証モードに変わったことを利用者が確認してから、端末1の方で、認証ボタンで認証申請し（ステップS306）、その結果として、認証通知を経て（ステップS307）、認証受領という動作になる（ステップS308）。上記の登録・認証シーケンス1、2とは異なり、この登録・認証シーケンス3では、利用者による端末1の認証ボタンの操作が実行される（ステップS305）。ステップS306の認証申請情報は、図20に示すように、認証申請要求、端末1のMACアドレス、そして、端末固有情報を含んでいる。これらのデータは、端末1の公開鍵方式の秘密鍵を用いて暗号化され、端末1から基地局Aへ送信される。ここで

注目すべきは、端末1の秘密鍵が使用されていることである。したがって、この鍵と対を成している公開鍵を利用しないと復号できない。これは、端末1によるデジタル署名である。このデジタル署名によって、時刻dまでに登録完了済みの端末1が送出した認証申請情報かどうかを判定することができる。

【0058】図19は、基地局Aと端末1との間で交換される情報に焦点をあてて、図18の登録・認証シーケンス3を説明するものである。図19の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス3では、端末1から基地局Aへ登録申請情報、認証申請情報および認証受領情報が無線通信される。また、基地局Aから端末1へ登録確認情報および認証通知情報が無線通信される。

【0059】この第3の実施例は、上記の第2の実施例と同様、認証通知と端末の認証モードへの切り替わりとの相関が明確なため、所望でない端末の誤った登録・認証を防止できる。

【0060】以上説明したように、この第3の実施例によれば、基地局Aの登録ボタンを操作してから、基地局Aのタイマ1がタイムアウトする前に、端末1の登録ボタンを操作する必要があり、また、端末1が認証モードに切り替わった後、基地局Aのタイマ2がタイムアウトする前に、端末1の認証ボタンを操作する必要がある。このため、家屋内にある基地局Aを外から操作することが困難なことから、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0061】(第4の実施例)次に、図21および図22を用いて、本発明の実施の形態に係る無線通信システムの第4の実施例を説明する。図21は、この第4の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図22は、基地局Aと端末1との間で交換される情報に焦点をあてて、図21の登録・認証シーケンス(登録・認証シーケンス4)を説明するものである。図22に示された丸囲み数字は、登録・認証シーケンス4の進行順を示している。この登録・認証シーケンス4では、端末1から基地局Aへ登録申請情報、認証申請情報および認証受領情報が無線通信される。また、基地局Aから端末1へ登録受付情報、登録確認情報および認証通知情報が無線通信される。以下、図21を参照して、この登録・認証シーケンス4を説明する。

【0062】(a) まず、利用者は、端末1の登録ボタンを押す(時刻a、ステップS401)。つまり、端末1の方から先に登録モード(LED表示は赤色点灯)に移行する。この時、タイマ3がスタートする。

【0063】(b) 次に、利用者は、基地局Aの登録ボタンを押す(時刻b、ステップS402)。登録ボタンが押されると、基地局Aは、図23に示す登録受付情報を、端末1へ送信する(ステップS403)。この時、基地局Aは、登録モードに移行し、そのLED表示は赤

色点灯となる。また、同時に、タイマ1もスタートする。図23に示すように、登録受付情報には、登録受付可能を示すフラグ、および、基地局MACアドレスが含まれる。

【0064】(c) 基地局Aからの登録受付情報を端末1が受信すると、今度は、端末1が、上記の図4に示した登録申請情報を基地局Aへ送信する(ステップS404)。

【0065】(d) 端末1からの登録申請情報を基地局Aが受信すると、基地局Aが、上記の図5に示した登録確認情報を端末1へ送信する(ステップS405)。この時、基地局Aのモードは登録モードから認証モードに切り替わる。また、タイマ1が正常終了すると共に、タイマ2がスタートする。基地局Aから送信される登録確認情報は、上記の第1の実施例で述べたように、登録申請した端末1の公開鍵で暗号化されているので、端末1だけがその内容を読むことができる。

【0066】(e) 端末1は、基地局Aからの登録確認情報を正しく復号できると、上記の図20に示した認証申請情報を基地局Aへ送信する(ステップS406)。この時、端末1のモードは、登録モードから認証モードに切り替わる。また、タイマ3が正常終了し、タイマ4がスタートする。図20の認証申請情報は、端末1の秘密鍵を用いて暗号化されているので、この鍵と対を成している公開鍵を利用しないと復号できない。これは、端末1によるデジタル署名と考えることができる。この署名によって、認証申請情報が、上記の(a)乃至(d)によって登録完了した端末1が送出したものであるか否かを判定することができる。

【0067】(f) 基地局Aは、端末1の公開鍵を知っているため、端末1からの認証申請情報を復号することができる。そして、基地局Aは、上記の図6に示した認証通知情報を端末1へ送信する(ステップS407)。この認証通知情報は、端末1の公開鍵で暗号化されており、その鍵と対を成している秘密鍵によって復号される。

【0068】(g) この復号によって、基地局Aの秘密鍵などを正しく取り出せると、上記の図7に示した認証受領情報を基地局Aへ送信する(ステップS408)。この時、端末1は(登録済み)通常モードになり、タイマ4も正常終了する。

【0069】(h) 端末1からの認証受領情報が基地局Aで受理されると、基地局Aも通常モードに戻り、タイマ2も正常終了する。ここで、端末1の登録・認証が完了する。

【0070】以上説明したように、この第4の実施例は、上記の第1乃至第3の実施例と異なり、全体の処理が基地局A主導であるという特徴がある。この第4の実施例によれば、端末1の登録ボタンを操作してから、端末1のタイマ3がタイムアウトする前に、基地局Aの登

録ボタンを操作する必要がある。このため、家屋内にある基地局Aを外部から操作することが困難なことに合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0071】（第5の実施例）次に、図24および図25を用いて、本発明の実施の形態に係る無線通信システムの第5の実施例を説明する。図24は、この第5の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図24の登録・認証シーケンス（登録・認証シーケンス5）が上記の第4の実施例の登録・認証シーケンス4と異なる点は、時刻fで端末1が認証申請情報を基地局Aへ送信する際、認証ボタンを利用することである。このようにすると、利用者が、端末1が登録モードから認証モードに切り替わったことを確認した後で、端末1の認証ボタンで認証申請することができる。上記の登録・認証シーケンス4と比べると、認証ボタンの分だけ手間が増すが、利用者に認証動作をより意識させる効果がある。

【0072】図25は、基地局Aと端末1との間で交換される情報に焦点をあてて、図24の登録・認証シーケンス5を説明するものである。図25の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス5では、端末1から基地局Aへ登録申請情報、認証申請情報および認証受領情報が無線通信される。一方、基地局Aから端末1へ登録受付情報、登録確認情報および認証通知情報が無線通信される。

【0073】この第5の実施例によれば、端末1の登録ボタンを操作してから、端末1のタイマ1がタイムアウトする前に、基地局Aの登録ボタンを操作する必要がある。また、端末1が認証モードに切り替わった後、基地局Aのタイマ2がタイムアウトする前に、端末1の認証ボタンを操作する必要がある。このため、家屋内にある基地局Aを外部から操作することが困難なことに合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0074】（第6の実施例）次に、図26および図27を用いて、本発明の実施の形態に係る無線通信システムの第6の実施例を説明する。図26は、この第6の実施例に係る無線通信システムの登録・認証シーケンスチャートである。図26の登録・認証シーケンス（登録・認証シーケンス6）が上記の第5の実施例の登録・認証シーケンス5と異なる点は、時刻fで端末1ではなく基地局Aの方で、認証ボタンを利用する点である。この操作によって、基地局Aが上記の図6に示した認証通知情報を端末1に送信する。登録・認証シーケンス5のように端末1が認証申請情報を送信する必要がない。つまり、端末1が登録モードから認証モードに切り替わったことを確認した後で、基地局Aの認証ボタンを押すということが、認証申請情報の送信に取って代わっている。また、第4の実施例の登録・認証シーケンス4との比較

では、認証ボタンの分だけ手間が増すが、利用者に認証動作をより意識させる効果がある。

【0075】図27は、基地局Aと端末1との間で交換される情報に焦点をあてて、図26の登録・認証シーケンス6を説明するものである。図27の丸囲み数字は登録・シーケンスの進行順を示すものである。この登録・認証シーケンス6では、端末1から基地局Aへ登録申請情報および認証受領情報が無線通信される。基地局Aから端末1へ登録受付情報、登録確認情報および認証通知情報が無線通信される。

【0076】この第6の実施例によれば、端末1の登録ボタンを操作してから、端末1のタイマ1がタイムアウトする前に、基地局Aの登録ボタンを操作する必要がある。また、端末1が認証モードに切り替わった後、端末1のタイマ4がタイムアウトする前に、基地局Aの認証ボタンを操作する必要がある。このため、家屋内にある基地局Aを外部から操作することが困難なことに合わせ、無線通信によりながらもセキュアかつ容易な登録・認証の処理を実施できる。

【0077】（無線基地局）次に、本発明の実施の形態に係る無線通信システムに適用される無線基地局について説明する。図28は、本発明の実施の形態に係る無線基地局のシステム構成を示すブロック図である。図28に示すように、この基地局10は、状態設定部101と、状態表示部102と、システム認証情報管理部103と、端末認証情報管理部104と、タイマ設定部105と、無線通信部106と、コントローラ107と、を備えている。

【0078】状態設定部101は、登録モードや認証モードのボタンである。状態表示部102は、たとえば、上記の第1乃至第6の実施例で述べたLED表示である。また、LED表示以外としては、液晶などの表示画面へのインストラクション表示、LEDの脇に印刷された文字列による指示、音声による指示、メロディによる表示、ネットワーク接続された他ノード画面へのインストラクション表示なども考えられる。

【0079】システム認証情報管理部103は、この基地局10の管轄システム内で使用される共通鍵暗号方式を管理する。共通鍵暗号方式の秘密鍵と暗号アルゴリズムとが管理されており、外部から容易には読み出せないようにしておく必要がある。端末認証情報管理部104では、この基地局10が管轄するシステムにおいて登録・認証済みの端末について、端末固有情報と公開鍵と暗号アルゴリズムとが、上記の図9に示した登録認証テーブルに管理されている。なお、基地局10自体の、端末としての、端末固有情報と公開鍵暗号方式の情報も管理されている。

【0080】タイマ設定部105は、上記の第1乃至第6の実施例で登場した基地局10のタイマを管理しており、そのスタートや終了を制御する。無線通信部106



は、無線により端末と情報の交換を行う部分である。

【0081】（無線端末）次に、本発明の実施の形態に係る無線通信システムに適用される無線端末について説明する。図29は、本発明の実施の形態に係る無線端末のシステム構成を示すブロック図である。図29に示すように、この端末20は、状態設定部201と、状態表示部202と、システム認証情報管理部203と、端末情報管理部204と、タイマ設定部205と、無線通信部206と、コントローラ207と、を備えている。

【0082】状態設定部201は、図28の状態設定部101と同様、登録モードや認証モードのボタンである。状態表示部202は、図28の状態表示部102と同様、たとえば、LED表示である。システム認証情報管理部203は、登録・認証を受けた基地局の管轄システム内の共通鍵暗号方式を保存する。共通鍵暗号方式の秘密鍵と暗号アルゴリズムとが管理されており、図28のシステム認証情報管理部103と同様、外部から容易には読み出せないようにしておく必要がある。端末情報管理部204は、この端末20の固有情報と公開鍵暗号方式の情報とを管理している。タイマ設定部205は、上述の実施例1〜6で登場した端末20のタイマを管理しており、そのスタートや終了を制御する。無線通信部206は、無線により基地局と情報の交換を行う部分である。

【0083】さて、上記の第1乃至第6の実施例の登録・認証シーケンス1乃至6を用いれば、基地局が管理するシステムに端末を登録・認証することが可能であることを説明してきた。本発明のように、ボタンなどのマニュアル操作と、LEDなどによる状態表示と、公開鍵方式と、共通鍵方式とを組み合わせると、通常の方法と同じ無線方式で登録・認証を行うことができ、成功したか失敗したか状態表示されるので利用者が容易に判断でき、また、外部から家屋内の基地局をマニュアル操作することは困難であるので、無線通信によりながらも、セキュアかつ容易な登録・認証が実施できる。

【0084】また、家庭内無線システムでは、基地局を複数用意して、個人やグループや家族全員など任意の単位で、柔軟に設定できると望ましいと考えられるが、これにも対応可能である。たとえば、図30のようなケースである。1軒の家（X家と呼ぶ）の中には、A氏専用の基地局Aと、B氏専用の基地局Bと、家族全員用の基地局Xとが設置されている。基地局Aは、A氏の端末3だけを登録・認証する。一方、基地局Aエリア内の、屋外の通りすがりの端末2や、B氏用端末4の登録・認証は拒否する。同様にして、基地局Bには、B氏の端末4だけが登録・認証される。基地局Xは、X家にある全端末を登録・認証するものであって、端末3や端末4だけでなく、基地局Aや基地局Bも端末として登録・認証する。なお、このような場合、端末の通常モードは1種類で、端末は複数の基地局に登録・認証することが可能と

なっている。また、このような場合、各端末には、複数基地局の共通鍵暗号方式の秘密鍵と暗号アルゴリズムが、システム認証情報蓄積部に管理されるようになる。たとえば、端末3には、基地局Aと基地局Xの秘密鍵と暗号アルゴリズムが管理される。

#### 【0085】

【発明の効果】本発明によれば、家庭内無線通信システムにおいて確実かつ容易な登録・認証を実行できる無線端末、無線基地局、家庭内無線通信システム、および、登録・認証方式を実現できる。

#### 【図面の簡単な説明】

【図1】本発明に係る無線通信システムを説明する図である。

【図2】本発明に係る登録・認証方法の第1の実施例を示すシーケンスチャートである。

【図3】基地局Aと端末1との間で交換される情報に焦点をあてて、図2のシーケンスチャートを説明する図である。

【図4】登録申請情報の内容を説明する図である。

【図5】登録確認情報の内容を説明する図である。

【図6】認証通知情報の内容を説明する図である。

【図7】認証受領情報の内容を説明する図である。

【図8】本発明に係る無線通信システムにおける登録・認証後の端末間での通信データの内容を説明する図である。

【図9】基地局の登録認証テーブルの内容を説明する図である。

【図10】図2のシーケンスチャートのタイマの動作を説明する図である（その1）。

【図11】図2のシーケンスチャートのタイマの動作を説明する図である（その2）。

【図12】図2のシーケンスチャートのタイマの動作を説明する図である（その3）。

【図13】図2のシーケンスチャートのタイマの動作を説明する図である（その4）。

【図14】図2のシーケンスチャートのタイマの動作を説明する図である（その5）。

【図15】本発明に係る登録・認証方法の第1の実施例において登録・認証が1回につき1端末限定であることを説明する図である。

【図16】本発明に係る登録・認証方法の第2の実施例を示すシーケンスチャートである。

【図17】基地局Aと端末1との間で交換される情報に焦点をあてて、図16のシーケンスチャートを説明する図である。

【図18】本発明に係る登録・認証方法の第3の実施例を示すシーケンスチャートである。

【図19】基地局Aと端末1との間で交換される情報に焦点をあてて、図18のシーケンスチャートを説明する図である。

【図20】認証申請情報の内容を説明する図である。

【図21】本発明に係る登録・認証方法の第4の実施例を示すシーケンスチャートである。

【図22】基地局Aと端末1との間で交換される情報に焦点をあてて、図21のシーケンスチャートを説明する図である。

【図23】登録受付情報の内容を説明する図である。

【図24】本発明に係る登録・認証方法の第5の実施例を示すシーケンスチャートである。

【図25】基地局Aと端末1との間で交換される情報に焦点をあてて、図24のシーケンスチャートを説明する図である。

【図26】本発明に係る登録・認証方法の第6の実施例を示すシーケンスチャートである。

【図27】基地局Aと端末1との間で交換される情報に焦点をあてて、図26のシーケンスチャートを説明する図である。

【図28】本発明に係る無線基地局の概略構成図である。

【図29】本発明に係る無線端末の概略構成図である。

【図30】本発明に係る他の無線通信システムを説明する

図である。

【図31】IEEE802.11WEPアルゴリズムにおける暗号化アルゴリズムを示す図である。

【図32】IEEE802.11WEPアルゴリズムにおける通信データフレームを示す図である。

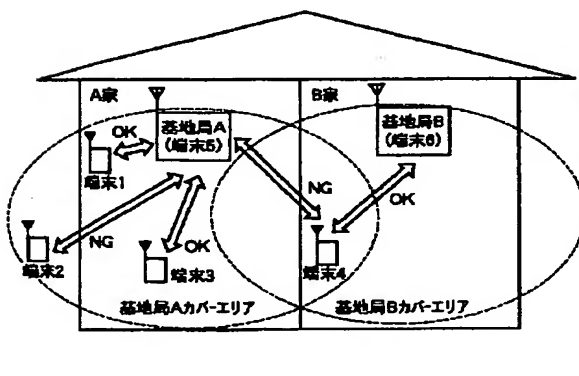
【図33】IEEE802.11WEPアルゴリズムにおける復号化アルゴリズムを示す図である。

【図34】IEEE802.11WEPアルゴリズムによる認証のシーケンスチャートである。

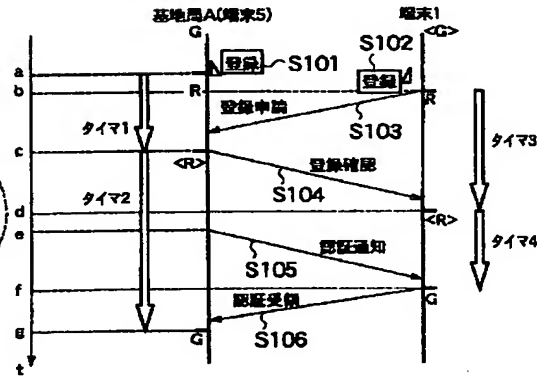
【符号の説明】

- 10 無線基地局
- 20 無線端末
- 101, 201 状態設定部
- 102, 202 状態表示部
- 103, 203 システム認証情報管理部
- 104 端末認証情報管理部
- 105, 205 タイマ設定部
- 106, 206 無線通信部
- 107, 207 コントローラ
- 204 端末情報管理部

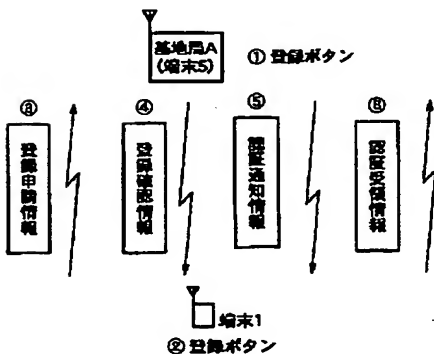
【図1】



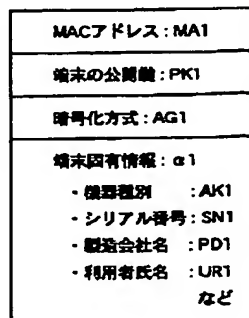
【図2】



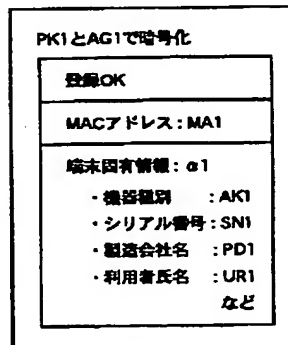
【図3】



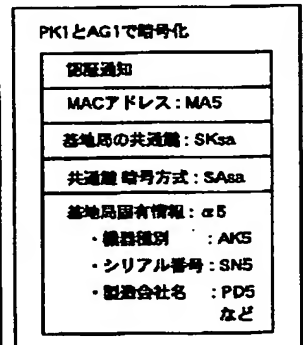
【図4】



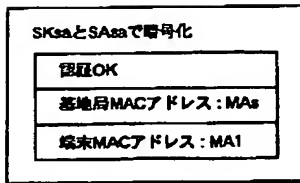
【図5】



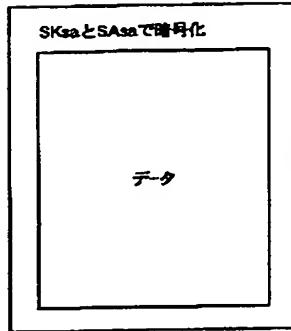
【図6】



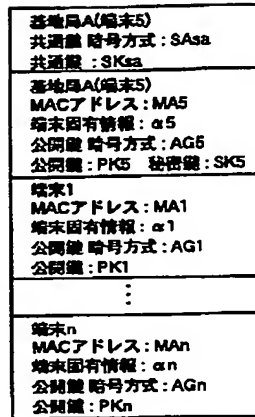
【図7】



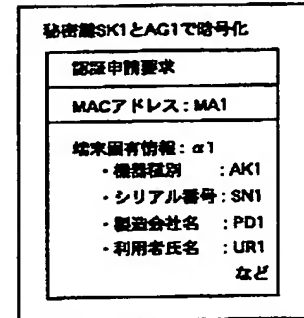
【図8】



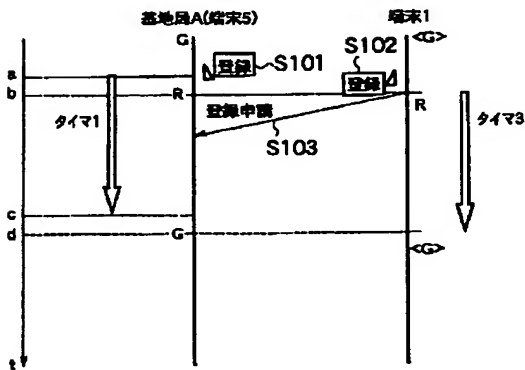
【図9】



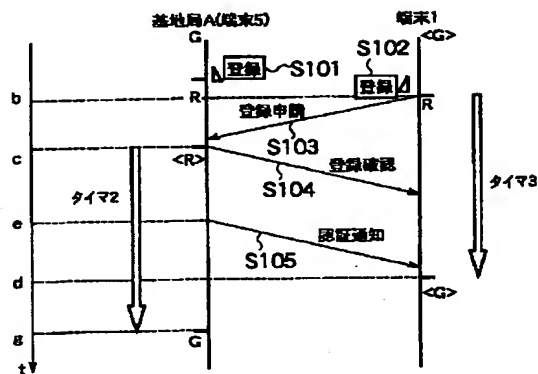
【図20】



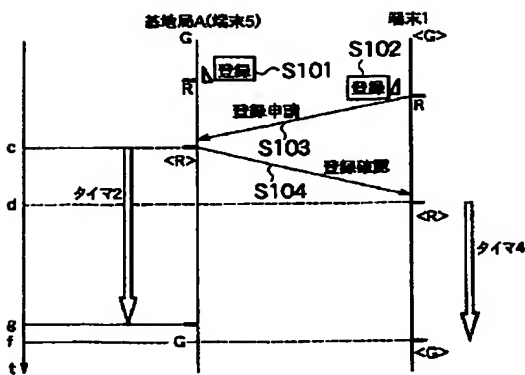
【図10】



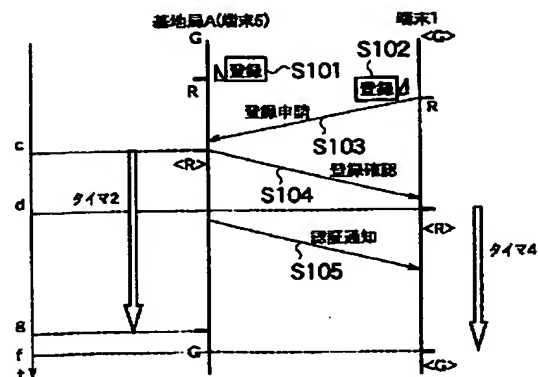
【図11】



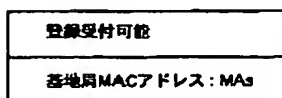
【図12】



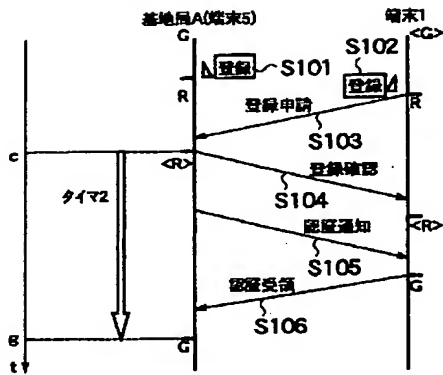
【図13】



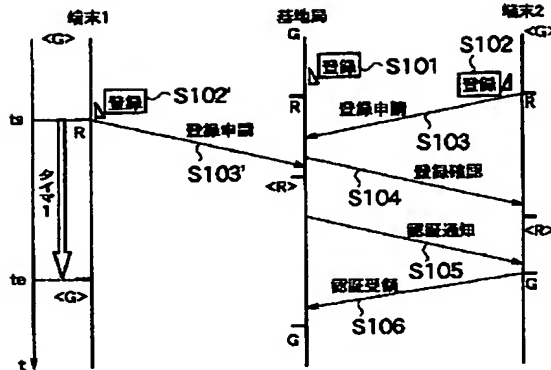
【図23】



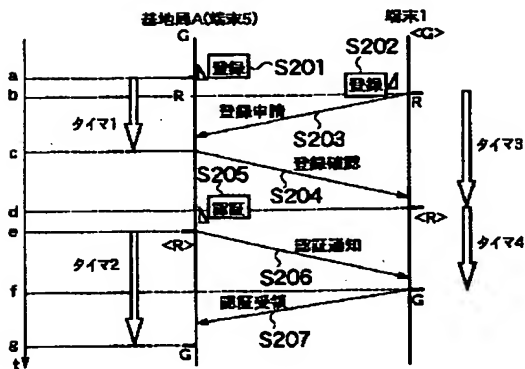
【図14】



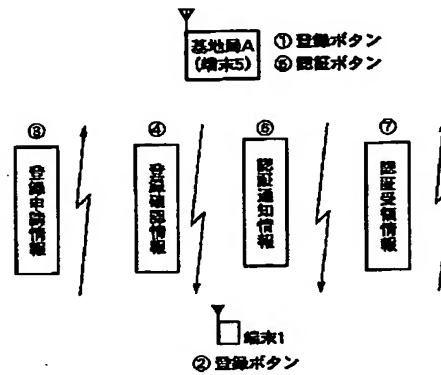
【図15】



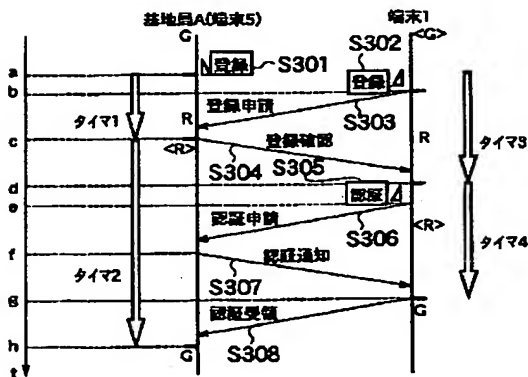
【図16】



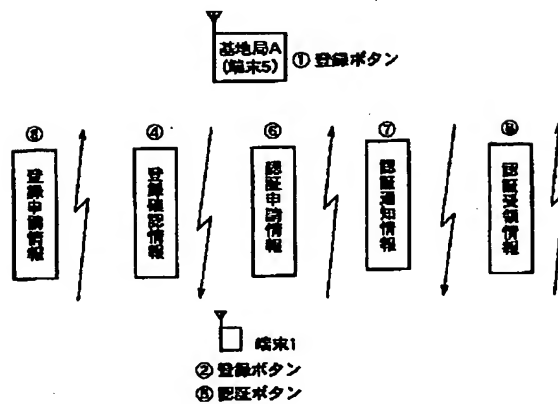
【図17】



【図18】



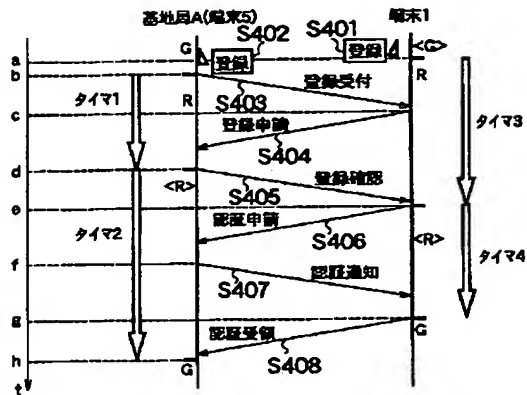
【図19】



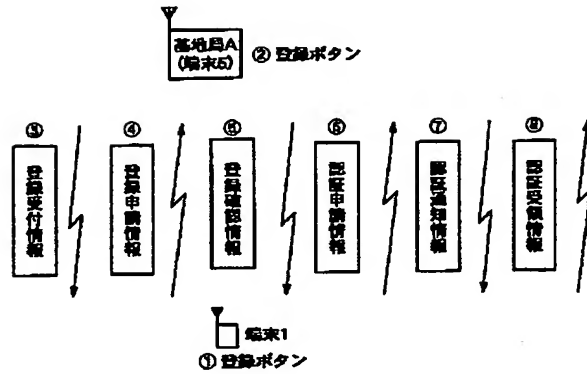
【図22】

IV	制御 コード	ET (PT)	0CV)
----	-----------	------------	------

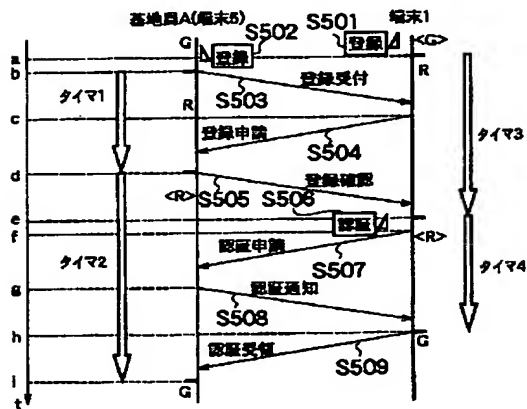
【図21】



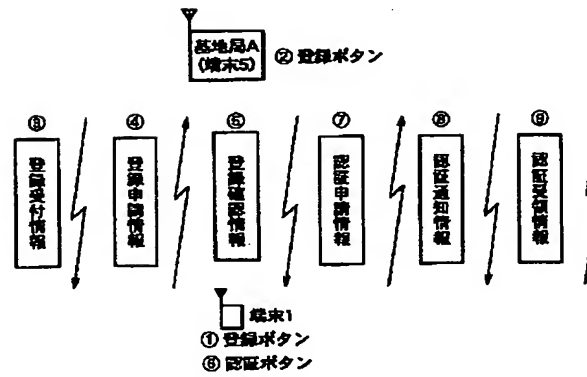
【図22】



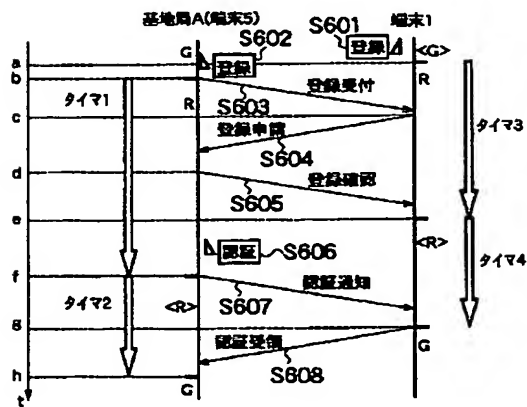
【図24】



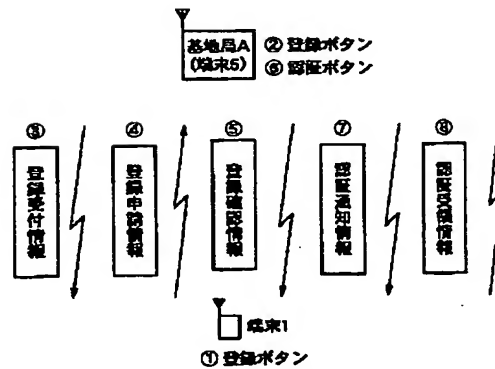
【図25】



【図26】

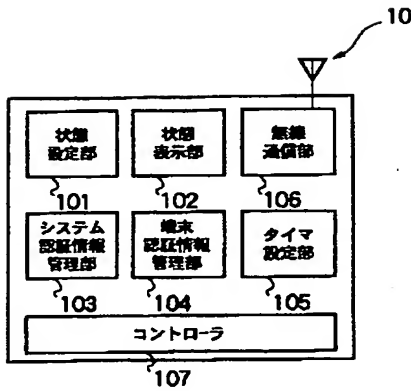


【図27】

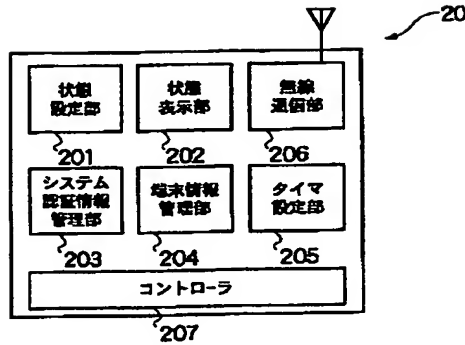




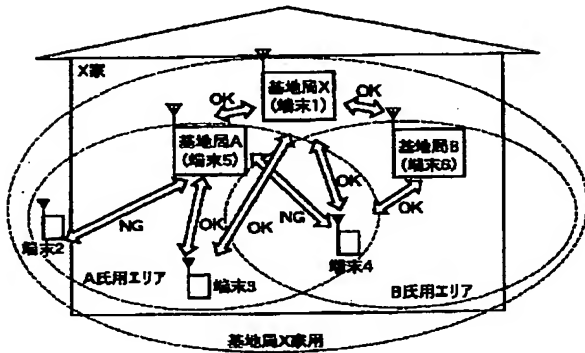
【図28】



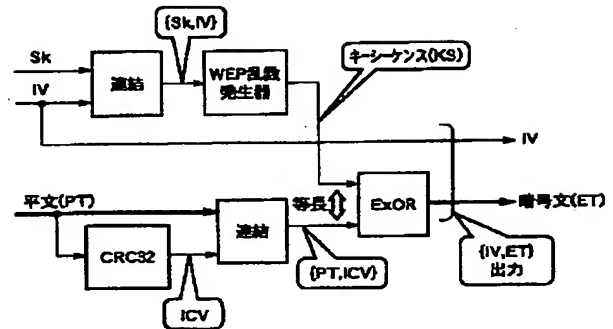
【図29】



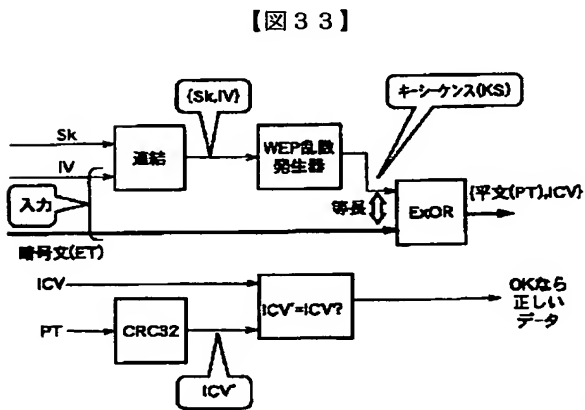
【図30】



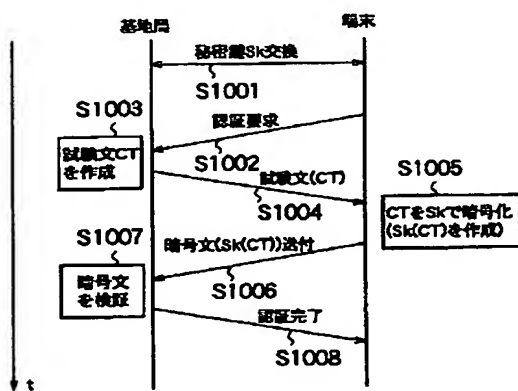
【図31】



【図34】



【図33】



フロントページの続き

Fターム(参考) 5J104 AA07 AA16 EA06 EA19 EA22  
JA03 KA02 KA05 KA09 NA02  
NA37 PA02  
5K033 AA08 BA01 CC02 DA01 DA19  
5K067 AA30 BB21 DD17 DD51 EE02  
EE10 FF05 HH36